Seminar Nasional Informatika 2008 (semnasIF 2008) *ISSN: 1979-2328*
UPN "Veteran" Yogyakarta, 24 Mei 2008

EVALUASI SISTEM INFORMASI TABUNGAN BANK UMUM

Noerlina N.,S.
Jurusan Komputerisasi Akuntansi Bina Nusantara University Jakarta
Jl. KH syahdan No. 9 Kemanggisan Jakarta Barat Telp.(021) 53696954
Email : noerlina@binus.edu

Abstrak
Perkembangan perekonomian perlu didukung oleh lembaga keuangan yang kokoh untuk menunjang kelancaran perekonomian. Bank sebagai salah satu lembaga keuangan adalah badan usaha yang menghimpun dana dari masyarakat dalam bentuk simpanan dan menyalurkan kepada masyarakat dalam bentuk kredit dan atau bentuk-bentuk lainnya dalam rangka meningkatan taraf hidup masyarakat banyak. Dalam menghadapi perkembangan perekonomian, kemajuan ilmu pengetahuan, teknologi dan informasi, serta tuntutan masyarakat akan layanan yang cepat dan aman, bank memerlukan pengelolaan yang baik, efektif dan efisien. Oleh karena itu diperlukan adanya sebuah sistem informasi yang andal yang dapat membantu pengelolaan aktivitas perbankan. Tujuan penelitian ini adalah mengidentifikasi efektivitas dan efisiensi sistem informasi tabungan yang berjalan dan memberikan rekomendasi yang dapat mengatasi kelemahan-kelemahan yang teridentifikasi. Metodologi penelitian yang digunakan adalah metode penelitian kepustakaan dan penelitian lapangan yang terdiri dari observasi, wawancara, check list, dan studi dokumentasi. Lingkup evaluasi yang dilakukan atas sistem informasi tabungan dari aspek pengendalian manajemen dan pengendalian aplikasi yang meliputi boundary, input, dan output. Berdasarkan evaluasi yang dilakukan, dapat ditarik simpulan bahwa pengendalian manajemen keamanan dan pengendalian input belum cukup baik karena ditemukan cukup banyak kelemahan, sedangkan pengendalian manajemen operasional, pengendalian batasan, dan pengendalian output sudah baik.

***Kata kunci** : Evaluasi, Sistem Informasi, Tabungan*

1. PENDAHULUAN

Perkembangan perekonomian perlu didukung oleh lembaga keuangan yang kokoh untuk menunjang kelancaran perekonomian. Bank sebagai salah satu lembaga keuangan adalah badan usaha yang menghimpun dana dari masyarakat dalam bentuk simpanan dan menyalurkan kepada masyarakat dalam bentuk kredit dan atau bentuk-bentuk lainnya dalam rangka meningkatan taraf hidup masyarakat banyak. Dalam menghadapi perkembangan perekonomian, kemajuan ilmu pengetahuan, teknologi dan informasi, serta tuntutan masyarakat akan layanan yang cepat dan aman, bank memerlukan pengelolaan yang baik, efektif dan efisien.

Sistem informasi dapat membantu pengelolaan aktivitas perbankan. Sistem informasi membantu mengumpulkan, mengelola, menyimpan, mengubah, serta memelihara data dan informasi perusahaan agar dapat akurat, relevan, cepat, dan lengkap. Dimana informasi tersebut nantinya diberikan kepada pemakai sebagai dasar pengambilan keputusan. Sistem informasi dapat dikatakan baik apabila memperhatikan kebutuhan pemakai baik itu data, informasi, maupun tampilannya, serta memerlukan pengawasan terhadap penggunaannya, selain itu juga harus dapat menunjang pelayanan dengan maksimal dan aman dari kemungkinan penyalahgunaan.

Sistem informasi tabungan yang digunakan berfungsi untuk mengumpulkan dan mengolah data tabungan nasabah serta mengeluarkannya dalam bentuk laporan. Karena begitu pentingnya sistem informasi tabungan bagi perusahaan untuk mendukung jalannya operasional sehari-hari, maka evaluasi terhadap sistem informasi tabungan dianggap perlu dengan tujuan adalah untuk mengetahui apakah sistem informasi tabungan yang berjalan telah efektif dan efisien bagi perusahaan.

2. TINJAUAN PUSTAKA

Tabungan

Pengertian tabungan menurut Undang-undang Perbankan nomor 10 tahun 1998 adalah simpanan yang penarikannya hanya dapat dilakukan menurut syarat-syarat tertentu yang disepakati, tetapi tidak dapat ditarik dengan cek, bilyet giro dan atau alat lainnya yang dipersamakan dengan itu.

Sistem Informasi Tabungan

Sistem informasi tabungan adalah kombinasi manusia, perangkat keras, perangkat lunak, jaringan komunikasi dan sumber daya data yang berfungsi untuk mengumpulkan, mengubah dan menyebarkan informasi tabungan yang bermanfaat bagi perusahaan.

Sistem Pengendalian Intern pada Sistem Berbasis Komputer

Dalam sistem pengendalian intern pada sistem berbasis komputer terdapat dua kategori pengendalian, yaitu pengendalian manajemen dan pengendalian aplikasi.

1. Pengendalian Manajemen

Pengendalian manajemen bertujuan untuk mengevaluasi apakah manajemen telah diatur dengan baik. Pengendalian manajemen terdiri dari :

a. Pengendalian Manajemen Keamanan

Pengendalian manajemen keamanan bertanggung jawab untuk menjamin keamanan aset sistem informasi. Ancaman utama terhadap keamanan aset sistem informasi antara lain :

1) Ancaman kebakaran
2) Ancaman air
3) Perubahan tegangan sumber energi
4) Kerusakan strukural
5) Polusi
6) Penyusup
7) *Viruses* dan *worms*
8) Penyalahgunaan *software*, data, dan *service*

b. Pengendalian Manajemen Operasional

Pengendalian manajemen operasional bertanggung jawab pada jalannya fasilitas perangkat keras dan perangkat lunak sehari-hari agar sistem aplikasi produksi dapat menyelesaikan pekerjaan dan pegawai dapat mendesain, mengimplementasikan serta menjaga sistem aplikasi. Tanggung jawab manajemen operasional yaitu :

1) Operasional komputer
2) Persiapan dan *entry* data
3) Pengendalian produksi
4) *File library*
5) *Documentation and program library*
6) *Help desk/technical support*
7) *Capcity planning and performance monitoring*

2. Pengendalian Aplikasi

Pengendalian aplikasi bertujuan untuk memastikan bahwa setiap aset sistem aplikasi dijaga, menjaga integritas data serta mencapai tujuan dengan efektif dan efisien. Pengendalian aplikasi terdiri dari :

a. Pengendalian Batasan

Subsistem batasan menentukan hubungan antara pengguna dengan sistem informasi. Pengendalian batasan terdiri dari :

1) Pengendalian *cryptographic*
2) Pengendalian akses
3) *Personal Identification Number* (PIN)
4) Tanda tangan digital
5) Kartu plastik
6) Pengendalian jejak audit

b. Pengendalian *Input*

Subsistem *input* bertanggung jawab memasukkan data dan instruksi ke dalam sistem aplikasi. Pengendalian *input* terdiri dari :

1) Metode *input* data
2) Desain dokumen sumber
3) Desain layar pemasukan data
4) Pengendalian kode data
5) *Check digit*
6) Pengendalian *batch*
7) Validasi data *input*
8) Pengendalian jejak audit

c. Pengendalian *Output*

Subsistem *output* menyediakan fungsi yang menentukan isi dari data yang akan disampaikan kepada pengguna, cara data disajikan kepada pengguna, cara menyiapkan data serta cara pengiriman data tersebut kepada pengguna. Pengendalian *output* terdiri dari :

1) *Inference control*
2) *Batch output production and distribution control*
3) *Batch report design control*
4) Pengendalian jejak audit

Audit Sistem Informasi

Menurut Weber (1999, p10), audit sistem informasi adalah proses mengumpulkan dan mengevaluasi bukti-bukti untuk menentukan kemampuan sistem komputer dalam melindungi aset, menjaga integritas data, mencapai tujuan organisasi dengan efektif dan menggunakan sumber daya dengan efisien.

Tahapan audit sistem informasi yaitu :

1. Perencanaan audit
   Bagi auditor eksternal hal ini berarti menginvestigasi klien untuk mengetahui apakah perjanjian audit dapat diterima, menempatkan staf audit yang layak, mendapatkan latar belakang klien, mengerti masalah hukum klien dan menganalisa prosedur agar dapat mengerti bisnis klien dengan baik dan mengidentifikasi resiko audit.
2. Pengujian pengendalian
   Auditor menguji pengendalian saat mereka menilai bahwa resiko pengendalian berada di bawah level maksimum.
3. Pengujian transaksi
   Mengevaluasi apakah terdapat kesalahan atau proses yang tidak biasa yang mengakibatkan kesalahan pencatatan yang material pada informasi keuangan.
4. Pengujian saldo atau hasil secara keseluruhan
   Pengujian saldo akhir untuk mendapatkan bukti yang cukup untuk dapat membuat keputusan akhir dari kehilangan atau kesalahan pernyataan laporan yang terjadi saat fungsi sistem informasi tidak dapat melindungi aset, menjaga integritas data dan mencapai efektivitas dan efisiensi sistem.
5. Penyelesaian audit
   Auditor eksternal melakukan beberapa pengujian tambahan terhadap bukti-bukti hingga selesai dan membuat opini tentang apakah terdapat kehilangan yang material atau kesalahan pernyataan laporan dan menerbitkan laporan.

3. METODE PENELITIAN

Metodologi penelitian yang digunakan dalam penelitian ini adalah :

1. Penelitian Kepustakaan
2. Penelitian Lapangan

Penelitian lapangan dilakukan dengan cara :

a. Observasi
b. Wawancara
c. *Check list*
d. Studi dokumentasi

Adapun metode analisa data yang digunakan pada penelitian ini yaitu metode kualitatif**.**

4. HASIL DAN PEMBAHASAN

Setelah dilakukannya evaluasi pada sistem informasi tabungan dihasilkan bahwa:

1. Pengendalian manajemen keamanan belum cukup baik karena cukup banyak ditemukan kelemahan, antara lain pada ancaman kebakaran, ancaman air, perubahan tegangan sumber energi, polusi, ancaman penyusup, ancaman virus, serta penyalahgunaan *software*, data, dan *service*
2. Pengendalian manajemen operasional sudah baik karena tidak ditemukan kelemahan pada pengendalian ini.
3. Pengendalian batasan sudah baik karena tidak ditemukan kelemahan pada pengendalian ini.
4. Pengendalian *input* cukup baik karena ditemukan beberapa kelemahan, antara lain sering terjadi salah input dan *response time* sistem tidak stabil.
5. Pengendalian *output* sudah baik karena ridak ditemukan kelemahan pada pengendalian ini..

Hasil Temuan Evaluasi :

1. Pengendalian Manajemen
   a. Pengendalian Manajemen Keamanan

Tabel 1. Pengendalian Manajemen Keamanan

No.	Temuan Evaluasi	Resiko	Rekomendasi
1.	Tidak terdapat alarm kebakaran otomatis di ruangan kantor.	Lambat mendeteksi adanya kebakaran, sehingga tingkat kebakaran dapat menjadi lebih tinggi.	Meletakkan alarm otomatis di seluruh ruangan, khususnya ruang *server*.
2.	Tidak terdapat alat pemadam kebakaran otomatis.	Jika terjadi kebakaran, pemadamannya lebih lambat sehingga api cepat menjalar ke seluruh ruangan.	Meletakkan alat pemadam otomatis di tempat - tempat yang strategis, khususnya di tempat aset sistem informasi berada.
3.	Tidak seluruh bangunan terbuat dari bahan tahan api.	Tingkat kebakaran menjadi lebih tinggi.	Menaruh alarm kebakaran dan alat pemadam kebakaran di tempat-tempat yang tidak terbuat dari bahan tahan api.
4.	Ruang *server* terbuat dari bahan tahan api, tetapi dilapisi *wallpaper* yang tidak tahan api.	*Server* hangus/rusak sehingga dapat menimbulkan kerugian seperti data hilang, biaya, dan terhentinya kegiatan operasional perusahaan.	Melepaskan *wallpaper* di ruang *server* dan menggantinya dengan cat.
5.	Peralatan pemadam kebakaran tidak diuji secara rutin.	Tidak dapat digunakan jika terjadi kebakaran.	Merawat dan menguji alat pemadam kebakaran secara rutin. Perawatan dan pengujian dapat dilakukan oleh pegawai perusahaan ataupun diserahkan ke pihak luar.
6.	Tidak seluruh perangkat keras ditutup dengan bahan tahan air jika tidak digunakan.	Perangkat keras akan rusak jika terkena air dan akan menyebabkan kerugian seperti data hilang, biaya harus yang dikeluarkan untuk memperbaiki/ mengganti perangkat keras yang rusak, dan pekerjaan pegawai terhambat.	Menutup seluruh perangkat keras dengan bahan tahan air saat tidak digunakan.
7.	Tidak terdapat peraturan yang jelas mengenai larangan merokok didalam ruangan dan larangan menaruh makanan dan minuman di dekat perangkat keras.	Merokok di dalam ruangan akan menyebabkan polusi dan perangkat keras dapat rusak jika terkena makanan dan minuman.	Membuat peraturan larangan merokok di dalam ruangan dan larangan menaruh makanan dan minuman di dekat perangkat keras secara tertulis.

Tabel 2. Lanjutan Pengendalian Manajemen Keamanan

8.	Perusahaan telah memiliki *stabilizer*, UPS, dan generator tetapi terkadang rusak, sehingga aliran listrik terganggu dan mati	Terhentinya kegiatan operasional perusahaan, kehilangan data dan rusaknya perangkat keras.	Merawat *stabilizer*, UPS, dan generator secara rutin. Perawatan dapat dilakukan oleh pegawai perusahaan ataupun diserahkan ke pihak luar. Meningkatkan daya listrik.
9.	Kamera keamanan / CCTV tidak aktif karena rusak.	Tingkat keamanan rendah karena penyusup dan hal-hal yang tidak diinginkan dapat terjadi.	Memperbaiki kamera keamanan/CCTV. Merawat kamera

			keamanan/CCTV secara rutin atau memberikan pemeliharaan kamera keamanan/CCTV ke pihak ketiga.
10.	Tidak terdapat kamera keamanan/CCTV di ruang *server*.	Tidak dapat mengetahui adanya tindak kejahatan dan pelakunya pada ruangan *server*.	Meletakkan kamera keamanan/CCTV di ruangan *server*.
11.	Pelatihan mengenai bahaya virus tidak diberikan secara berkala.	Perkembangan virus yang semakin banyak dan cepat tidak dapat diantisipasi, sehingga perusahaan dapat kehilangan data.	Memberikan pelatihan mengenai bahaya virus, tindakan pencegahan, dan tindakan mengatasi virus kepada pegawai secara berkala.
12.	Tidak terdapat alarm keamanan.	Lambat mengetahui adanya tindak kejahatan/ penyusup, sehingga tingkat kerugian perusahaan (kehilangan barang-barang/uang, dan menurunnya tingkat kepercayaan nasabah) menjadi lebih besar.	Meletakkan alarm keamanan di setiap pintu keluar dan jendela bangunan.

b. Pengendalian Manajemen Operasional

Tidak terdapat temuan pada pengendalian manajemen operasional.

2. Pengendalian Aplikasi

a. Pengendalian Batasan

Tidak terdapat temuan pada pengendalian batasan.

c. Pengendalian *Input*

Tabel 3. Pengendalian Input

No.	Temuan Evaluasi	Resiko	Rekomendasi
1.	Tidak terdapat pembedaan warna pada tampilan layar.	Salah meng-*input* data, salah memilih menu, yang dapat menyebabkan kerugian materil maupun waktu bagi pihak nasabah atau perusahaan.	Memberikan pengarahan kepada pegawai agar lebih berhati-hati dan lebih teliti saat meng-*input* data.
2.	*Response time* tidak stabil, karena tergantung jumlah transaksi.	Waktu pegawai bekerja menjadi lebih lama.	Menambah kapasitas memori, membuat peraturan dimana pengguna tidak diperbolehkan mengambil atau menggunakan data yang berukuran besar pada saat jam sibuk, serta memberikan pelatihan kepada operator agar lebih tanggap saat jam sibuk.

d. Pengendalian *Output*

Tidak terdapat temuan pada pengendalian *output*.

5. KESIMPULAN

1. Peningkatan pada pengendalian manajemen keamanan dengan cara menyediakan alarm kebakaran dan alat pemadam kebakaran otomatis, merawat dan menguji alat pemadam kebakaran, melepas *wallpaper* di ruang *server*, menutup perangkat keras dengan bahan tahan air saat tidak digunakan, merawat *stabilizer*, UPS, dan generator secara rutin, serta memperbaiki dan meletakkan kamera keamanan/CCTV dan alarm keamanan di tempat yang strategis.

2. Pada pengendalian manajemen operasional, pengendalian batasan, dan pengendalian *output* agar perusahaan tetap mempertahankannya dan akan lebih baik lagi jika ditingkatkan secara terus-menerus.
3. Pada pengendalian *input* sebaiknya perusahaan menambah kapasitas memori, membuat peraturan dimana pengguna tidak diperbolehkan mengambil atau menggunakan data yang berukuran besar pada saat jam sibuk., serta memberikan pelatihan kepada operator agar lebih tanggap saat jam sibuk.

6. DAFTAR PUSTAKA

Arens, A.A dan Loebbecke, J.K. 2003. *Auditing Pendekatan Terpadu*. Edisi Indonesia. Terjemahan Amir Abadi Jusuf. Salemba Empat, Jakarta.

Bodnar, G.H dan Hopwood, W.S. 2000. *Sistem Informasi Akuntansi*. Buku Satu. Terjemahan Jusuf, A.A, dan Tambunan, R.M. Salemba Empat, Jakarta.

Gondodiyoto, Sanyoto. 2006. *Audit Sistem Informasi + Pendekatan CobIT*. Edisi Revisi. Mitra Wacana Media, Jakarta.

Indriantoro, N dan Supomo, B. 2002. *Metodologi Penelitian Bisnis Untuk Akuntansi dan Manajemen*. Edisi ke-1. BPFE, Yogyakarta.

Jones, F.L dan Rama, D.V. 2006. *Accounting Information System : A Business Process Approach*. Thomson South-Western, Kanada.

Kasmir. 2004. *Manajemen Perbankan*. PT RajaGrafindo Persada, Jakarta.

O'Brien, J.A. 2005. *Introduction to Information System Essentials for the e-Business Enterprise*. Edisi 12. McGraw Hill Companies, Inc, United State.

Undang-undang nomor 10 tahun 1998.

Weber, Ron. 1999. *Information Systems Control and Audit*. Prentice-Hall, Inc, New Jersey.